THE COMPLEXITIES OF CENTRAL ASIAN

CYBER SECURITY

Turkmen officials receive laptop computers at a ceremony in Ashgabat in July 2013. Turkmenistan has recently allowed its citizens greater access to the Internet. AFP/ GETTY IMAGES

THE FIGHT AGAINST INTERNET CRIME MUST NOT NEGLECT DEMOCRATIC PRINCIPLES

By Nuria Kutnaeva, independent researcher, Kyrgyz Republic

After obtaining independence in 1991, Kazakhstan, the Kyrgyz Republic, Tajikistan, Turkmenistan and Uzbekistan — all facing completely new challenges and threats to their national securities — each chose different paths for political, social and economic development. Border security, religious extremism, drug trafficking, corruption and political turbulence have been longstanding problems in Central Asian states, but a new challenge surfaced in the last decade: crime involving high-technology and the Internet.

Cyber security is closely connected to the spread of the Internet, which is growing throughout Central Asia, despite varying connection speeds. In terms of Internet speed, Kazakhstan was ranked 58th out of 188 countries in February 2014, Tajikistan was 66th, the Kyrgyz Republic 81st and Uzbekistan 171st,[1] according to Ookla, a company that tests broadband speeds every 30 days. The average download speed in the European Union was rated as much faster.

In 2010, Kazakhstan had the highest rate of infected computers and spam traffic among the five Central Asian states (85 percent).[2] And in 2013, 92 percent of Kazakh organizations experienced at least one cyber attack.[3] This was likely due to the large number of Internet users and Kazakhstan's attractive financial state. Kazakhstan was followed by Uzbekistan with 8 percent and the Kyrgyz Republic with 4 percent of infected computers. Tajikistan (1 percent) and Turkmenistan (2 percent) had the lowest percentage of infected and spammed computers.[4]

CYBER CRIME IN CENTRAL ASIA

Cyber crime falls into three major categories in Central Asia: hooliganism, hacktivism and cyber fraud. Cyber hooliganism implies "muscle-flexing" — done by young, talented hackers[5] who want to prove to colleagues how easily they can disrupt a system. On July 19, 2010, a 14-year-old boy from Russia and his friends hacked into the website of the National Space Agency of Kazakhstan by creating a user account with administrator rights. The boy argued that the developers did not sufficiently protect the portal. "What we did is, of course, illegal," the boy said in justification. "But on the Kazakhstani website, we created a topic where we indicated where its vulnerability is."[6]

Since the Internet is a symbol of globalization, hackers become comfortable operating internationally. The Central Asian states suspect they are victims of foreign hackers because defaced[7] or cracked websites are sometimes left with images of foreign flags and inscriptions. However, the origin is unknown. Cyber security specialist Oleg Demidov of the PIR Center in Moscow points out that hackers from around the world often redirect attacks to hide their identity or to pin the blame on others.[8]

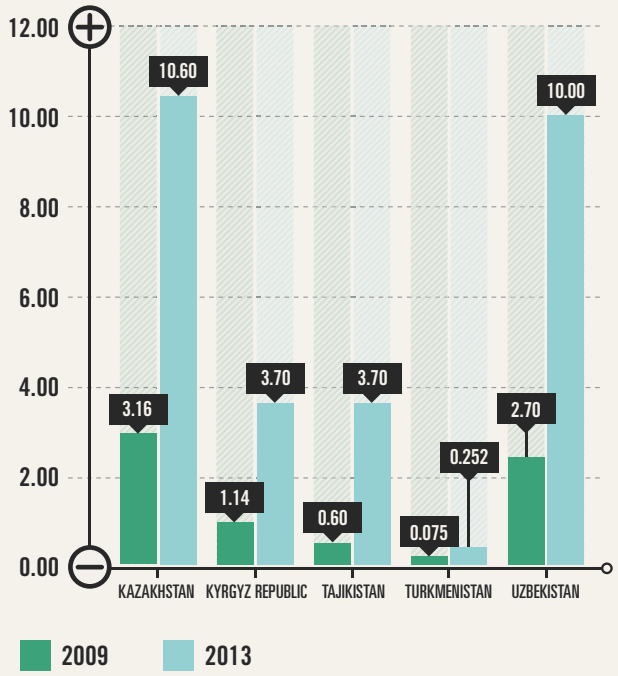
For example, in 2012-2013, several Kyrgyz government sites were vandalized by hackers believed to be from Turkey and Estonia. In 2012, a hacker from Turkey changed the passwords to many Kazakh websites.[9] In 2013, a Malaysian or Indonesian team hacked nine Kazakh legal websites. They left a message calling for the liberation of Palestine.[10]

Competition and revenge are often motivators. For example, in 2011 a Kazakh website selling cars was hit with severe distributed denial-of-service (DDoS) attacks. Owners of the site concluded that revenge was the motive because site administrators had declared war against fraudsters who had tried to sell cheap cars through their site.[11]

Hacktivism, the act of hacking or breaking into a computer system for political or social reasons, occurs frequently in Central Asia. As Ty McCormick, editor at *Foreign Policy* magazine, puts it: "If there's one thing that unites hacktivists across multiple generations, its dedication to the idea that information on the Internet should be free — a first principle that has not infrequently put them at odds with corporations and governments the world over."[12]

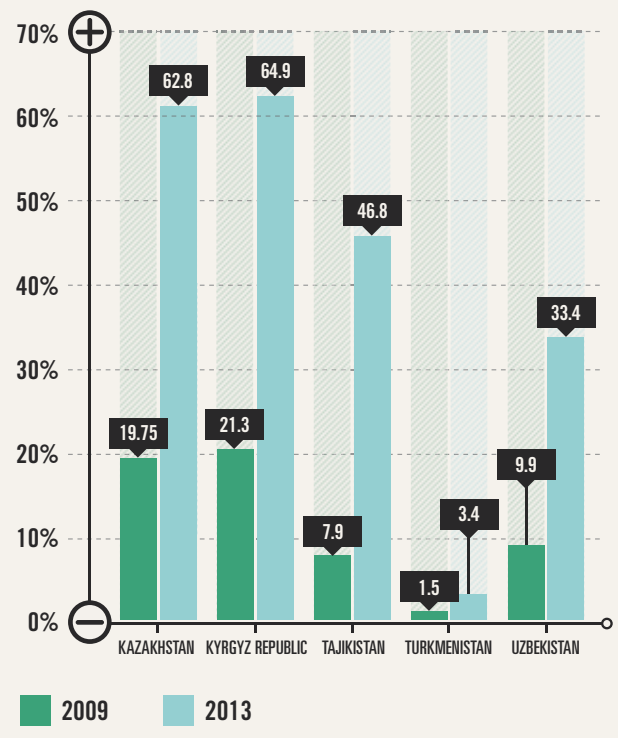
Hacktivists in Central Asia are frequently individuals or groups of information technology (IT) specialists whose main motivation is political: They want to bring an issue to the attention of their government. An Uzbek case is illustrative. In early 2013, there were two defacing attacks on the official website of the national television and radio broadcasting company of Uzbekistan, MTRK. Uzbek hackers, calling themselves

GRAPH 1. ***Number of Internet users (in millions)***



Sources: Profit.kz, ZAKON.kz, *Vecherniy Bishkek*, Internet World Stats

GRAPH 2. ***Proportion of Internet users to a country's population (percentage)***



Sources: *Demoscope Weekly*, Kaspersky Lab

PER CONCORDIAM ILLUSTRATION

"Clone-Security," made the following public statement: "This is a political action, called 'Anti-lying' ['Antilagman']. This company disseminates false information to the people. The people are not satisfied with the transmissions of the national television and radio broadcasting company. For example, the events associated with the closure of the [cellular company] MTS are not covered by MTRK. At one point, millions of people were left without communications. But no information was available. Website Olam.uz constantly talked about MTS, but stopped today. The events on the Kyrgyz-Uzbek border and the tragedy in Sokh happened — and no information from MTRK. And even non-governmental channels are under strict control."[13]

The same hacking team was responsible for defacing the Ministry of Healthcare's website in 2012; they disagreed with the government's policy on forced sterilization of women. The defaced website had an inscription: "Stop sterilizing our moms. Clone-Security."[14]

This group also has foreign policy ambitions. In February 2013, it launched attacks against Kyrgyz government and public websites. Cyber criminals left the inscription: "Clone Security: We are against racism," with the Uzbekistan flag in the background. Human rights violations against ethnic Uzbeks in the Kyrgyz Republic served as the impetus for the attack.[15]

Cyber fraud is cyber crime committed in the financial sphere. For example, in 2009, a 20-year-old Kazakh IT specialist hacked into the computer system of a Kazakh bank and transferred $1 million to his bank account. He fled to Moscow, where Russian police arrested him after he attempted to withdraw the money.[16]

Governmental institutions are not exempt from fraudsters, nor are non-financial businesses. In a case of cyber extortion, on March 9, 2012, the owner of a Kyrgyz entertainment website suffered several days of DDoS attacks. A hacker sent a blackmail message warning that the attacks would continue if the owner didn't pay.[17] In Tajikistan in December 2013, the court convicted three cyber criminals who converted international calls into internal calls and stole the rate difference.[18]

SILENCING OPPOSITION

Sometimes Central Asian governments block access to pro-opposition websites by organizing DDoS attacks against them, producing a considerable challenge to Central Asian societies. Most revealingly, in February 2005 two major Internet providers in the Kyrgyz Republic found themselves under DDoS attack. The Kyrgyz government blocked sites that presented an alternative to government versions of current politics. A site specializing in Central Asian issues, periodically under DDoS attacks, received a letter demanding they stop reporting on the situation in the Kyrgyz Republic.

The first Kyrgyz revolution happened on March 24, 2005. Two weeks later, the site administration received an

email from a Ukrainian confessing to organizing the DDoS attacks. He explained his motives this way:

In early February 2005, a man identifying himself as a Kyrgyz patriot contacted the Ukrainians, saying that parliamentary elections were upcoming and that several websites were writing about the authorities' malevolence and slandering the president and his family. He asked the Ukrainians if they could block selected websites during the elections. "Now we see what happened in Kyrgyzstan — the madness of the crowd, looting, bloodshed. ... We think that it is also a consequence of the fact that people did not have access to truthful information. We consider ourselves responsible for those riots that took place in Kyrgyzstan," the hacker admitted. "We have only now realized the full impact of our actions in suppressing information. We are ready to come to Bishkek, speak at a press conference, tell everything we know and return the money to the Kyrgyz people."[19]

Kazakhtelecom, Kazakhstan's biggest telecommunications provider, controls about 70 percent of the country's broadcast market. In 2010, Radio Free Europe/Radio Liberty reported that some Kazakh nongovernmental organization websites were blocked.[20] As of January 2014, several pro-opposition websites were still denied in Kazakhstan. Authorities used the same method to block the website of the portal "Republic" (http://www.respublika-kz.info/).[21] In February 2009, opposition-minded websites such as zona.kz, geo.kz, and respublika.kz suffered massive DDoS-attacks. Kazakh government officials called on Google to withdraw some of the Internet content from their search results. In 2012, there were four requests to delete 40 items, and 75 percent of these requests were fulfilled.[22] In the first half of 2013, there were three requests to delete 209 items from the Internet, and Google fulfilled 67 percent of these requests.[23]

Likewise, in Tajikistan in 2012, 30 websites known to post material critical of the current authorities of Tajikistan were blocked. A number of Russian news sites could not be accessed as well.[24] On the eve of presidential elections in November 2013, Tajik authorities blocked the site of the Tajik news agency Ozodagon, its Russian version on catoday.org, and the video-hosting site YouTube.[25]

Uzbekistan and Turkmenistan possess the most restrictive policies on public access to the Internet. According to OpenNet, a multinational project that monitors and reports on Internet filtering and surveillance, both states hold the highest level of Internet censorship.[26] Blocking and dropping connection speeds for certain sites — the reason behind low Internet speeds in Uzbekistan — are common practices that the Uzbek government uses to target the opposition. Authorities ordered Internet service providers to block several hundred websites in Uzbekistan.[27] In Turkmenistan, the situation is even worse; there is only one Internet service provider, TurkmenTelekom.[28] In Ashgabat, the capital of Turkmenistan, fewer than 10 Internet cafes operate. Users are required to show passports, and identifying information is recorded by Internet cafe administrators.[29]

GOVERNMENT AGENCIES CONFRONT CYBER CHALLENGES

Special units inside ministries of internal affairs pay close attention to cyber crimes. For example, the "K" Department established in the Ministry of Internal Affairs of Kazakhstan in April 2003[30] contends with a wide range of crimes connected with computer and Internet technology, including cyber bullying, counterfeit DVDs,[31] spread of information promoting extremism, terrorism, cruelty and violence, and child pornography. In 2006, Kazakh authorities established the

1. A Kyrgyz woman in traditional dress speaks on a mobile phone. The people of Central Asian countries are rapidly embracing new communications technologies, necessitating a greater emphasis on cyber security.

2. Turkmen troops guard an Internet cafe in Ashgabat. Internet use in Turkmenistan is highly controlled, and all online activity is recorded by Internet cafe administrators.

REUTERS

REUTERS

AGENCE FRANCE-PRESSE

Children use computers in Ashgabat, capital of Turkmenistan. President Gurbanguly Berdymukhamedov has broadened the country's use of the Internet since his inauguration in 2007.

National Contact Point to fight IT crime and to exchange information with the Commonwealth of Independent States and foreign partners.[32]

In the Kyrgyz Republic, a group focusing on cyber threats was established inside the Ninth Main Directorate of the Ministry of Internal Affairs in 2009. Its main objective is to search for the online presence of extremist organizations, such as Hisb-ut-Tahrir.[33] In Tajikistan, cyber criminals were recently caught by the Directorate for Combating Organized Crime.[34]

Other governmental entities specializing in communications and technologies are also responsible for meeting cyber threats. This is the case in Uzbekistan, where the Computer Emergency Response Team (UZ-CERT) was started in 2005. And in September 2013, the Information Security Center was launched within the State Committee of Communication, Information System Development and Telecommunication Technologies.[35] In Tajikistan, the government communications service is very powerful and reportedly blocked dozens of sites in 2012 and 2013.

RESPONDING TO CYBER THREATS

Realizing that defending against cyber threats demands cooperation with other international stakeholders, regional leaders have raised issues of information security within the framework of regional organizations. At the summit of the Shanghai Cooperation Organization (SCO) in 2006, heads of member states signed the Declaration on International Information Security. In 2009, participants in the SCO summit in Yekaterinburg, Russia, adopted the Yekaterinburg Declaration, which underscores the urgent need to respond to cyber threats. In the SCO, information security was deemed as important as national sovereignty, national security, and social and economic stability.

At the latest SCO summit, in Bishkek in 2013, Kazakh President Nursultan Nazarbayev stated that his country supported the improvement of activities within the SCO Regional Anti-Terrorist Structure (RATS). We "welcome the first meeting of experts on cyberterrorism held in June of this year in Tashkent."[36] To counter information threats, it was decided to establish from SCO member states an expert group on international information security.[37]

In 2010, the Collective Security Treaty Organization (CSTO) adopted the Regulation on Cooperation in the Field of Information Security. The purpose is to create an institutional and legal framework for cooperation among the members of the organization. CSTO performs a range of operations called "Countering Criminals in Information." Its main objective is to combat cyber crime in member states and to counteract prohibited information on the Internet relating to extremism, terrorism and information that can cause political damage to states' interests. For example, during operations in 2009-2010, more than 2,000 websites were identified as inciting ethnic and religious hatred, and more than 600 sites were suspended.[38] During the latest operation, conducted in 2013 in the southern Kyrgyz Republic, about a dozen sites were accused of recruiting terrorists and inciting interethnic dissention.[39]

In September 2011, SCO states that included Russia, China, Tajikistan and Uzbekistan submitted a draft resolution to the United Nations General Assembly on information security.[40] The International Code of Conduct for Information Security proposed the regulation of state actions in cyberspace. Rules also called for UN member states to cooperate in combating criminal, terrorist, and extremist activities with the use of information resources, as well as any activity that "undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment."[41]

The rules specify that it is unacceptable to use information and communication technologies in a manner contrary to international security. The document sends three interesting messages. First, it declares that a threat with an unknown origin needs to be addressed. This threat may come from nonstate actors or other states. In fact, the rules identify "three evils": terrorism, secession and extremism, in line with the ability of other countries via information technologies "to carry out

hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies."[42] Second, the document confirms the right of every state to control and monitor Internet technologies on their territories: "to reaffirm all the rights and responsibilities of States to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage."[43] Third, it stipulates that cooperation between state and private companies is essential to combat cyber threats.

CONCLUSION

In the past decade, aside from economic, social and political challenges, Central Asian states had to contend with a threat no one expected back in 1991. Internet use has grown so fast in recent years that government authorities could not accommodate their responses to it adequately. Therefore, they reached for solutions based on familiar practices in the political and social spheres — by blocking Internet providers, obstructing Websites and tampering with Internet connection speeds.

At the moment — luckily enough — Central Asian states are confronted with threats only from the lowest levels of cyber crime — hooliganism, hacktivism and cyber fraud. However, in such a turbulent region, threats of cyber terrorism and cyber warfare should not be underestimated. Therefore, Central Asian governments must take active steps to protect their own critical information infrastructure.

Finally, declaratory statements and intentions to cooperate in cyberspace are made within the framework of Central Asian regional organizations. Identifying sites with extremist and terrorist content in each other's national domains is a great idea. However, it is a big question whether or not more in-depth cooperation is possible. It requires trust, and there should be a joint understanding of information security concepts. Hopefully, over time, understanding will grow on this issue and Central Asian states will move in a good democratic direction. □

1. No figures are given for Turkmenistan. Household Download Index, Ookla Net Index, January 15, 2014, http://www.netindex.com/download/allcountries/
2. Ekaterina Isakova, Hackers choose Kazakhstan, Kursiv.kz, October 21, 2010, http://www.kursiv.kz/news/details/hitech-weekly/xakery-vybirayut-kazaxstan/
3. Kazakhstan IT-specialists underestimate the seriousness of cyber threats. October 28, 2013. Profit.kz <http://profit.kz/news/10147/Kazahstanskie-IT-specialisti-nedoocenivaut-sereznost-kiberugroz/>
4. Ekaterina Isakova. Hackers choose Kazakhstan, Kursiv.kz, October 21, 2010, http://www.kursiv.kz/news/details/hitech-weekly/xakery-vybirayut-kazaxstan/
5. For the purposes of this article, we understand the general term "hacking" to be all illegal actions of access and intrusion to information resources without consent of their owners or administrators.
6. Kazakhstan: The hacker who cracked the site of Kazkosmos turned out to be a Russian schoolboy. March 15, 2012, International News Agency Fergana. http://www.ferganannews.com/news.php?id=18339
7. "Defacing" is changing the main page of the website without changing system files.
8. A personal correspondence between Oleg Demidov and the author. January 17, 2014.
9. Kazakh sites are attacked by Turkish hackers. May 16, 2012, Express-K, http://profit.kz/news/8526/Kazahstanskie-sajti-podvergautsya-atake-tureckih-hakerov/
10. Kazakh sites hacked from Southeast Asia, December 4, 2013, Profit.kz. http://profit.kz/news/11236/Kazahstanskie-sajti-vzlomani-hakerami-iz-Ugo-Vostochnoj-Azii/
11. Governmental sites of Kazakhstan are poorly protected from DDoS-attacks. December 4, 2012, Total.kz. http://profit.kz/news/9236/Gossajti-RK-slabo-zaschischeni-ot-DDoS-atak/
12. Ty McCormick. Hacktivism. *Foreign Policy*. May/June 2013, Issue 200, p. 24-25.
13. In Uzbekistan, the site MTRK was hacked. Ozodlik, 30 January 2013. http://www.ozodlik.org/content/article/24888716.html
14. Ibid.
15. Askat Turusbekov. Sites of Kyrgyz security agencies were hacked. Kabar, February 21, 2013. http://kabar.kg/incident/full/50072
16. Darura Zhalyn, A Hole in the Bank, *Businessweek*, June 12, 2009, http://profit.kz/articles/908/Dirka-v-banke/
17. Hacker attacks on websites of government agencies and the media in the Kyrgyz Republic (history). Tazabek, May 5, 2013 http://www.w.tazabek.kg/news:350162/
18. Tajikistan, for the first time, condemned the group of "hackers." Top News, December 28, 2013. http://www.topnews.tj/2013/12/28/v-tadzhikistane-vpervyie-osudili-gruppu-hakerov/
19. "Kyrgyz" hackers ready to arrive in Bishkek, require security guarantees - letter Central Asia. January 4, 2005. http://www.centrasia.ru/newsA.php?st=1112320800
20. NGO Says 14 Websites Being Blocked In Kazakhstan. Radio Free Europe/Radio Liberty. January 27, 2010, http://www.rferl.org/content/NGO_Says_14_Websites_Being_Blocked_In_Kazakhstan/1941642.html
21. Zarina Kozybayeva. What is lacking in the Internet in CA . May 7, 2010. Deutsche Welle. http://dw.de/p/NEDQ.
22. Google Report on the availability of services and data. January-June 2012 http://www.google.com/transparencyreport/removals/government/countries/?p=2012-06; July-December 2012. http://www.google.com/transparencyreport/removals/government/countries/?p=2012-12
23. Google Report on the availability of services and data. January-June 2013, http://www.google.com/transparencyreport/removals/government/countries/
24. Galim Faskhutdinov. Internet in Tajikistan is not developed, but the authorities are afraid of it. Deutsche Welle. December 5, 2012, http://dw.de/p/16vc8
25. Mehrangez Tursunzoda. In Tajikistan, the sites Ozodagon and YouTube are blocked. «ASIA-Plus». November 5, 2013. http://news.tj/ru/news/v-tadzhikistane-zablokirovali-saity-ozodagon-i-youtube
26. OpenNet Initiative. Country profiles: Uzbekistan, Turkmenistan. https://opennet.net/research/profiles
27. Uzbekistan: unlock some independent sites. Internet censorship has malfunctioned again? October 27, 2013. http://www.ferganannews.com/news/21412
28. Neither Here Nor There: Turkmenistan's Digital Doldrums. OpenNet Initiative. https://opennet.net/neither-here-nor-there-turkmenistan percentE2 percent80 percent99s-digital-doldrums
29. Personal interview with an Ashgabat inhabitant (on a confidential basis). January 11, 2014.
30. Oksana Koksegenova, Hackers threaten Kazakhstan, April 5, 2007, Kursiv.
31. Polina Krestovskaya. Watch out. Everything is recorded. Almanews.kz. April 27, 2009, http://profit.kz/articles/837/Akkuratno-Vse-zapisivaetsya/
32. Oksana Koksegenova, Hackers threaten Kazakhstan, April 5, 2007, Kursiv.
33. Jyldyzbek Ibraliev. Kyrgyz law enforcement agencies established a unit to fight cyber crime. January 12, 2009. Information Agency «24.kg», http://www.24.kg/community/2009/01/12/102859.html
34. In Tajikistan, for the first time condemned the group of "hackers." Top News, December 28, 2013. http://www.topnews.tj/2013/12/28/v-tadzhikistane-vpervyie-osudili-gruppu-hakerov/
35. The problems of information security are discussed. State Committee for Communications, Information and Telecommunication Technologies of the Republic of Uzbekistan. October 31, 2013, http://ccitt.uz/ru/press/aci_news/2013/10/932/. See also Resolution of the Cabinet of Ministers of September 16, 2013, No. 250, "On measures of organization the Center for Development of the 'E-government' and the Center for Information Security under the State Committee for Communication, Information and Communication Technologies of the Republic of Uzbekistan." http://www.pravo.uz/resources/anons/monitoring/files/pos_250.pdf
36. Kazakhstan supports the expansion of the functions of the Executive Committee of the SCO RATS by cyber terrorism and cyber crime – President. KAZINFORM. September 13, 2013. http://www.inform.kz/rus/article/2589151
37. CO RATS Council decides to establish a group to combat terrorism on the Internet. Novosti-Kazakhstan. September 20, 2013. http://newskaz.ru/politics/20130920/5567047.html
38. More than 2,000 extremist websites were detected in Russia for two years – Bordyuzha, RIA Novosti. December 21, 2010, http://ria.ru/defense_safety/20101221/311598350.html # ixzz2qugWwWn1
39. CSTO found in the southern Kyrgyz Republic sites to recruit terrorists. Rosbalt, March 28, 2013, http://www.rosbalt.ru/exussr/2013/03/28/1111069.html
40. Letter dated September 12, 2011, from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the secretary-general. 66th session, Item 93 of the provisional agenda, Developments in the field of information and telecommunications in the context of international security A/66/359, September 14, 2011, Developments in the field of information and telecommunications in the context of international security, http://daccess-ods.un.org/TMP/9878256.91699982.html
41. Ibid.
42. Ibid.
43. Ibid.